



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,782	03/03/2000	Kouya Tochikubo	04329.22444	7469

22852 7590 06/17/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER

ZIA, MOSSADEQ

ART UNIT	PAPER NUMBER
----------	--------------

2134

9

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/518,782

Applicant(s)

TOCHIKUBO ET AL.

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 March 2000.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 4,5,7-14 and 17-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 4,5,7-14 and 17-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. **Claims 4, 5, 7, 9, 11, 12, 13, 14, 18, 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,199,069, Barrett et al. in view of Patent Application Publication US 2000/0046564, Masuda et al. and in further view of Patent No. 6,249,866, Brundrett et al. and in further view of Patent No. 6,694,025, Epstein et al.**

3. Regarding claim 22, Barrett show a cryptographic communication terminal comprising:
a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication (Barrett, col. 3, line 58-60), outputting a designated cryptographic algorithm, said cryptographic algorithm storage section storing an encrypted cryptographic algorithm (synchronization, Barrett, col. 4, line 14-16, 29-31);

control means for designating , with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication (Barrett, col. 2, line 15-17; col. 3, line 54-56); and

encryption/decryption means for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section

Art Unit: 2134

and the key designated with respect to said key information storage section, and encrypting information to be transmitted (Barrett, col. 4, line 60-62; col. 5, line 21-23);

but fail to show:

(a) a cryptographic algorithm decryption means of decrypting the encrypted cryptographic algorithm;

(b) key information decryption means for decrypting an encrypted key from said key information storage section;

a key information storage section for storing a key used for cryptographic communication corresponding to the cryptographic algorithm, and outputting a designated key, said key information storage section storing a key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm

(c) as well as the key for cryptographic communication;

however,

a) Masuda shows a system where a medium for storing (algorithm storage section) an algorithm encrypted together with the data. A loader in the device driver 22 loads the encrypted algorithm 34 into the PC (terminal) 11, transmits it to the server 33 (decrypting means), and requested the server 33 to decrypt the algorithm 34. Then the loader 31 receives the algorithm decrypted by the server 33 and transmits it to the decrypting unit 23. The decrypting unit 23 decrypts the data according to transmitted algorithm (Masuda, fig. 6, pp. 2, para. 0046).

b) Brundrett teaches an encryption key that is a random number encrypted by the public key of at least one user and at least one recovery agent. These keys are stored with the files (key

Art Unit: 2134

information storage section), whereby the file can always be decrypted by the private key of either a user or a recovery agent (Brundrett, col. 2, line 41-44, col. 10, line 13-15).

c) Epstein teaches network system where the server contains a list of public/private key pairs, wherein the private key is stored in an encrypted form (Epstein, col. 3, line 63-65).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Masuda and Brundrett and Epstein to include encrypted decryption algorithm such that Barrett gains the advantage of further improving the security for the data stored on the storage medium (Masuda, pp. 1, para. 0017) and provide a strong cryptographic solution that addresses encryption data recovery (Brundrett, col. 2, line 21-22) and to provide a method for securely storing private keys in a networked environment (Epstein, col. 2, line 53-55).

4. Regarding claim 4, Barrett and Masuda and Brundrett and Epstein discloses claim 22 above, and further disclose the key for the encrypted algorithm is a key for secret key cryptography (encryption key, Brundrett, col. 2, line 41-44).

5. Regarding claim 5, Barrett discloses claim 22 above, and further disclose the key for the encrypted algorithm is a key for public key cryptography (Epstein, col. 3, line 64-65).

6. Regarding claim 7, Barrett and Masuda and Brundrett and Epstein disclose claim 22 above and further discloses said

control means instructs (controller, Barrett, col. 3, line 26-27) said cryptographic algorithm storage section to output a requested cryptographic algorithm (control signal, Barrett, col. 4, line 5-6) upon receiving a transmission request (binary signal, Barrett, col. 3, line 68, col.

4, line 1) for any one of the cryptographic algorithms stored in said cryptographic algorithm storage section, and

said encryption/decryption means encrypts the requested cryptographic algorithm as the information to be transmitted (Barrett, col. 4 , line 29-31, col. 7, line 66-68, col. 8, line 1-2).

7. Regarding claim 9, Barrett and Masuda and Brundrett and Epstein 22 above, and further show when the algorithm decryption key is requested from the partner, said apparatus inputs the corresponding algorithm decryption key as the information to be transmitted to the partner to said encryption/decryption means (Epstein, col. 4, line 49-53).

8. Regarding claim 13, Barrett disclose claim 22 above, and further shows a cryptographic communication system comprising not less than two cryptographic communication terminals (Barrett, col. 1, line 60-62).

9. Regarding claim 14, Barrett disclose claim 22 above, and further shows a cryptographic communication system comprising not less than one cryptographic communication terminals (Barrett, col. 1, line 60-62).

10. Regarding claim 20, Barrett and Masuda and Brundrett and Epstein shows claim 13 above, and further show cryptographic communication terminal acquires a cryptographic algorithm (Masuda, page 2, col. 2, para. 0046, last 2 lines) and a decryption key from said cryptographic communication center apparatus (Epstein, col. 4, line 22-24).

11. Regarding claim 21, Barrett and Masuda and Brundrett and Epstein shows claim 11 above and further show cryptographic communication terminal acquires a cryptographic algorithm from another terminal (Masuda, page 2, col. 2, para. 0046, last 2 lines) and acquires a

Art Unit: 2134

corresponding decryption key from said crypto communication center apparatus (Epstein, col. 4, line 22-24).

12. Regarding claim 23, Barrett show a computer readable medium storing a program for implementing:

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication (Barrett, col. 3, line 58-60), outputting a designated cryptographic algorithm, said cryptographic algorithm storage section storing an encrypted cryptographic algorithm (synchronization, Barrett, col. 4, line 14-16, 29-31);

control means for designating , with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication (Barrett, col. 2, line 15-17; col. 3, line 54-56); and

encryption/decryption means for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted (Barrett, col. 4, line 60-62; col. 5, line 21-23);

but fail to show:

(a) a cryptographic algorithm decryption means of decrypting the encrypted cryptographic algorithm;

(b) key information decryption means for decrypting an encrypted key from said key information storage section;

a key information storage section for storing a key used for cryptographic communication corresponding to the cryptographic algorithm, and outputting a designated key, said key information storage section storing a key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm

(c) as well as the key for cryptographic communication;

however,

a) Masuda shows a system where a medium for storing (algorithm storage section) an algorithm encrypted together with the data. A loader in the device driver 22 loads the encrypted algorithm 34 into the PC (terminal) 11, transmits it to the server 33 (decrypting means), and requested the server 33 to decrypt the algorithm 34. Then the loader 31 receives the algorithm decrypted by the server 33 and transmits it to the decrypting unit 23. The decrypting unit 23 decrypts the data according to transmitted algorithm (Masuda, fig. 6, pp. 2, para. 0046).

b) Brundrett teaches an encryption key that is a random number encrypted by the public key of at least one user and at least one recovery agent. These keys are stored with the files (key information storage section), whereby the file can always be decrypted by the private key of either a user or a recovery agent (Brundrett, col. 2, line 41-44, col. 10, line 13-15).

c) Epstein teaches network system where the server contains a list of public/private key pairs, wherein the private key is stored in an encrypted form (Epstein, col. 3, line 63-65).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett as per teaching of Masuda and Brundrett and Epstein to include encrypted decryption algorithm such that Barrett gains the advantage of further improving the security for the data stored on the storage medium (Masuda, pp. 1, para. 0017) and provide a

strong cryptographic solution that addresses encryption data recovery (Brundrett, col. 2, line 21-22) and to provide a method for securely storing private keys in a networked environment (Epstein, col. 2, line 53-55).

13. Regarding claim 18, Barrett and Masuda and Brundrett and Epstein shows claim 23 above, and show further when a key for the encrypted algorithm is requested from the partner, inputting the corresponding key for the encryption algorithm, as the information to be transmitted to the partner, to said encryption/decryption means (Brundrett, col. 2, line 41-44).

14. **Claims 8, 10, 17, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,199,069, Barrett et al. in view of Patent Application Publication US 2000/0046564, Masuda et al. and in further view of Patent No. 6,249,866, Brundrett et al. and in further view of Patent No. 6,694,025, Epstein et al. in further view of Patent No. 4,484,025, Ostermann et al.**

15. Regarding claim 8, Barrett and Masuda and Brundrett and Epstein shows claim 22 above, and further show a partner with which said terminal communicates is an apparatus including said cryptographic communication terminal (Barrett, col. 2, line 32-34), but fails to show said terminal requests the partner for a new cryptographic algorithm and/or a key for a corresponding encrypted algorithm, decrypts a corresponding response by using said encryption/decryption means, stores the requested cryptographic algorithm in said cryptographic algorithm storage section upon receiving the cryptographic algorithm, and stores the requested key for the encrypt algorithm in said key information storage section upon receiving the key.

However, Ostermann teaches a system for enciphering and deciphering data (Ostermann, fig. 1) where the system cipher algorithm is transmitted from the cipher program storage 18 over

a data transmission channel 20 to the program memory 22 of the programmable cipher computer (Ostermann, col. 2, line 38-41). It further shows that the transmission of a cipher program can also be initiated at the programmable cipher computer 12 by means of a cipher request initiator. This permits the transmitting terminal 1 to request that the cipher algorithm be transmitted from the receiving terminal 2 prior to transmission (Ostermann, col. 3, line 4-9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett and Masuda and Brundrett and Epstein as per teaching of Ostermann such that exchange of enciphered information without requiring the standardization of the cipher algorithms, and which makes it possible the continued use of already available ciphering devices (Ostermann, col. 1, line 40-43).

16. Regarding claim 10, Barrett and Masuda and Brundrett and Epstein shows claim 9 above, but fails to show an update cryptographic algorithm storage section for storing a plurality of types of cryptographic algorithms decrypted by using a key for the encrypted algorithm, and said control means, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructs said update cryptographic algorithm storage section, in place of said cryptographic algorithm storage section, to output the requested cryptographic algorithm as the information to be transmitted.

However Ostermann teaches that cipher algorithm (Ostermann, fig. 1) is transmitted from the cipher program storage (Ostermann, element 18) over a data transmission channel (element 20) to the program memory (Ostermann, col. 2, line 38-41). The data transmitted between the first and the second terminals is enciphered in accordance with the cipher program code and the cipher key stored in the programmable computer (Ostermann col. 1, line 64-68). Furthermore,

it shows that the storage computer is provided with a long-term memory for storage of a plurality of different cipher programs (Ostermann, col. 2, line 59-60).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett and Masuda and Brundrett and Epstein as per teaching of Ostermann such that exchange of enciphered information without requiring the standardization of the cipher algorithms, and which makes it possible the continued use of already available ciphering devices (Ostermann, col. 1, line 40-43).

17. Regarding claim 17, Barrett and Masuda and Brundrett and Epstein shows claim 23 above, but fails to show a transmission request for any the cryptographic algorithms stored in said cryptographic algorithms storage means is received, instructing said cryptographic algorithm storage means to output the requested cryptographic algorithm, and

said encryption/decryption means further comprises a program for encrypting the requested cryptographic algorithm as the information to be transmitted.

However Ostermann teaches that cipher algorithm (Ostermann, fig. 1) is transmitted from the cipher program storage (Ostermann, element 18) over a data transmission channel (element 20) to the program memory (Ostermann, col. 2, line 38-41). The data transmitted between the first and the second terminals is enciphered in accordance with the cipher program code and the cipher key stored in the programmable computer (Ostermann col. 1, line 64-68). Furthermore, it shows that the storage computer is provided with a long-term memory for storage of a plurality of different cipher programs (Ostermann, col. 2, line 59-60).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett and Masuda and Brundrett and Epstein as per teaching of Ostermann such that

Art Unit: 2134

exchange of enciphered information without requiring the standardization of the cipher algorithms, and which makes it possible the continued use of already available ciphering devices (Ostermann, col. 1, line 40-43).

18. Regarding claim 19, Barrett and Masuda and Brundrett and Epstein shows claim 23 above, and further show

means for, when the cryptographic algorithm decryption key is requested from the partner, inputting a corresponding key from the encrypted algorithm, as information to be transmitted to the partner, to said encryption/decryption means (Brundrett, col. 2, line 41-44), but fail to show

updating cryptographic algorithm storage means for storing a plurality of types of cryptographic algorithms encrypted by the key for the encrypted algorithm; and

wherein said control means stores a program for, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructing said update cryptographic algorithm storage means to output the requested cryptographic algorithm as the information to be transmitted.

However Ostermann teaches that cipher algorithm (fig. 1) is transmitted from the cipher program storage (element 18) over a data transmission channel (element 20) to the program memory (Ostermann, col. 2, line 38-41). The data transmitted between the first and the second terminals is enciphered in accordance with the cipher program code and the cipher key stored in the programmable computer (Ostermann col. 1, line 64-68). Furthermore, it shows that the storage computer is provided with a long-term memory for storage of a plurality of different cipher programs (Ostermann, col. 2, line 59-60).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Barrett and Masuda and Brundrett and Epstein as per teaching of Ostermann such that exchange of enciphered information without requiring the standardization of the cipher algorithms, and which makes it possible the continued use of already available ciphering devices (Ostermann, col. 1, line 40-43).

Response to Arguments

19. Applicant's arguments with respect to claim 4,5,7-14 and 17-23 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Art Unit: 2134


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
6/8/04


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100